F-Secure Anti-Virus 2013

çindekiler

Bölüm 1: Yükleme.....5

lk kez yüklemeden önce.....6
Ürünü ilk kez yükleme.....6
Uygulamaları yükleme ve yükseltme.....6
Yardım ve Destek.....7

Bölüm 2: Ba larken.....9

Otomatik güncelle tirmeler nasıl kullanılır.....10
Güncelle tirme durumunu denetleme.....10
Internet ba lantı ayarlarımı de i tirme.....10
Gerçek Zamanlı Koruma A ı'nın durumunu denetleme.....11
Ürününün neler yaptı ını görme.....11
Bildirim geçmi ini görüntüle.....11
Bildirim ayarlarını de i tirme.....11
Gerçek Zamanlı Koruma A ı.....12
Gerçek Zamanlı Koruma A ı nedir?.....12
Gerçek Zamanlı Koruma A ı'nın faydaları.....12
Hangi verilere katkıda bulunursunuz?.....13
Gizlili iniz nasıl korunuyor?.....14
Gerçek Zamanlı Koruma A ı katılımcısı olma.....14
Gerçek Zamanlı Koruma A ı ile ilgili sorular.....14
Aboneli imin geçerli oldu unu nasıl bilebilirim.....15
Eylem merkezi.....15
Aboneli i etkinle tir.....15

Bölüm 3: Giri 17

Genel koruma durumunuzu görüntüleme.....18
Ürün istatistiklerini görüntüleme.....18
Ürün güncelle tirmelerini i leme.....19
Veritabanı sürümlerini görüntüleme.....19
Cep telefonu geni bant ayarlarını de i tir.....19
Virüsler ve di er kötü amaçlı yazılımlar nedir.....20
Virüsler.....20
Casus yazılımlar.....20
Kendini gizleyen yazılımlar.....21
Riskli yazılımlar.....21

Bölüm 4: Kötü amaçlı yazılımlara kar ı bilgisayarı koruma.....23

Bilgisayarımı nasıl tarayabilirim.....24

Dosyaları otomatik olarak tarama.....24

Dosyaları elle tarama.....26

E-postaları tarama.....29

Tarama sonuçlarını görüntüleme.....29

Dosyalar nasıl taramanın dı ında bırakılır.....30

Dosya türlerini dı lama.....30

Konuma göre dosyaları dı lama.....31

Dı lanan uygulamaları görüntüleme.....31

Karantina nasıl kullanılır.....32

Karantinaya alınan ö eleri görüntüleyin.....32

Karantinaya alınan ö eleri geri yükleme.....33

DeepGuard nedir.....33

DeepGuard'ı açma veya kapatma.....33

DeepGuard'ın engelledi i uygulamalara izin verme.....34

DeepGuard'ı uyumluluk modunda kullanma.....34

üpheli davranı uyarılarıyla ne yapmak gerekir.....34

Bölüm

1

Yükleme

Konular:

- *Ik kez yüklemeden önce*
- *Ürünü ilk kez yükleme*
- *Uygulamaları yükleme ve yükseltme*
- *Yardım ve Destek*

Ik kez yüklemeden önce

F-Secure ürününü seçti iniz için te ekkür ederiz.

Ürünü yükleyebilmek için unlara ihtiyacınız vardır:

- Yükleme CD'si veya yükleme paketi. CD sürücüsü olmayan bir netbook kullanıyorsanız, yükleme paketini *www.f-secure.com/netbook* adresinden yükleyebilirsiniz.
- Abonelik anahtarınız.
- Internet ba lantısı.

Ba ka bir üreticiye ait bir güvenlik ürününüz varsa, yükleyici onu otomatik olarak kaldırmaya çalı acaktır. Bu gerçekle mezse, lütfen el ile kaldırın.

Not: Bilgisayarda birden fazla hesabınız varsa, yükleme i lemi için yönetici ayrıcalıklarıyla oturum açın.

Ürünü ilk kez yükleme

Ürünü yükleme yönergeleri

Ürünü yüklemek için u yönergeleri uygulayın:

1. CD'yi yerle tirin veya indirdi iniz yükleyiciyi çift tıklatın.

   CD otomatik olarak ba latılmazsa Windows Gezgini'ne gidin, CD-ROM simgesini ve yüklemeyi ba latmak için de yükleme dosyasını çift tıklatın.

2. Ekrandaki yönergeleri uygulayın.

   - Ürünü bir ma azadan CD olarak satın aldıysanız, abonelik anahtarını Hızlı Yükleme Kılavuzu kapa ında bulabilirsiniz.
   - Ürünü F-Secure eStore'dan yüklediyseniz, abonelik anahtarı satın alma sipari inin onay e-postasında bulunur.

   Aboneli inizi do rulamadan ve Internet'ten en son güncellemeleri yüklemeden önce bilgisayarınızın yeniden ba latılması gerekebilir. CD'den yüklüyorsanız, bilgisayarınızı yeniden ba latmadan önce Yükleme CD'sini çıkarmayı unutmayın.

Uygulamaları yükleme ve yükseltme

Yeni aboneli inizi etkinle tirme yönergeleri.

Yeni aboneli inizi etkinle tirmek veya ba latma ekranını kullanarak yeni bir uygulama yüklemek için u yönergeleri uygulayın:

Not: Ba latma ekranı simgesini Windows sistem tepsisinde bulabilirsiniz.

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Bir açılır menü ekrana gelir.
2. **Aboneliklerimi görüntüle**'yi seçin
3. **Aboneliklerim** altında, **Abonelik durumu** sayfasına gidin ve **Aboneli i etkinle tir**'i tıklatın.
   Aboneli i etkinle tir penceresi açılır.
4. Uygulama için abonelik anahtarınızı girin ve **Tamam**'ı tıklatın.

5. Aboneli iniz do rulandıktan ve etkinle tirildikten sonra, **Kapat**'ı tıklatın.
6. **Aboneliklerim** altında, **Yükleme durumu** sayfasına gidin. Yükleme otomatik olarak ba latılmazsa, u yönergeleri uygulayın:
   a) **Yükle**'yi tıklatın.
      Yükleme penceresi açılır.
   b) **leri**'yi tıklatın.
      Uygulama indirilir ve yükleme i lemi ba lar.
   c) Yükleme tamamlandı ında, **Kapat**'ı tıklatın.

Yeni abonelik etkinle tirilmi tir.

Yardım ve Destek

Ürün ekranında herhangi bir yerde Yardım simgesini tıklatarak veya F1'e basarak çevrimiçi olarak ürün yardımına eri ebilirsiniz.

Lisansınızı kaydettikten sonra, ücretsiz ürün güncellemeleri ve ürün deste i gibi ek hizmetler almaya hak kazanırsınız. *www.f-secure.com/register* adresinden kaydolabilirsiniz.

Bölüm

2

Ba larken

Konular:

- *Otomatik güncelle tirmeler nasıl kullanılır*
- *Ürününün neler yaptı ını görme*
- *Gerçek Zamanlı Koruma A ı*
- *Aboneli imin geçerli oldu unu nasıl bilebilirim*

Ürünü kullanmaya nasıl ba layaca ınız ile ilgili bilgiler.

Bu bölümde, ba latma paneli aracılı ıyla ortak ayarların nasıl de i tirilece i ve aboneliklerinizin nasıl yönetilece i açıklanır.

Ba latma panelinin ortak ayarları, ba latma panelinde yüklü olan tüm programlara uygulanan ayarlardır. Bu ayarları her bir program için ayrı ayrı de i tirmek yerine, yüklü olan tüm programlar tarafından kullanılan ortak ayarları düzenlemeniz yeterlidir.

Ba latma panelindeki ortak ayarlar unlardır:

- Kar ıdan Yüklemeler altından, kar ıdan yüklenmi güncelle tirmeler ile ilgili bilgileri görüntüleyebilir ve yeni güncelle tirmeler olup olmadı ını el ile denetleyebilirsiniz.
- Ba lantı ayarları altından, bilgisayarınızın Internet'e ba lanma biçimini de i tirebilirsiniz.
- Bildirimler altından, geçmi bildirimleri görüntüleyebilir ve hangi bildirim türlerini görmek istedi inizi ayarlayabilirsiniz.
- Gizlilik ayarları altından, bilgisayarınızın Gerçek Zamanlı Koruma A ı'na ba lanmasına izin verilip verilmedi ini seçebilirsiniz.

Yüklü programlar için aboneliklerinizi de ba latma paneli aracılı ıyla yönetebilirsiniz.

Otomatik güncelle tirmeler nasıl kullanılır

Otomatik güncelle tirmeler bilgisayarınızın korumasını güncel tutar.

Ürün, Internet'e ba lı oldu unuzda en yeni güncelle tirmeleri bilgisayarınıza alır. A trafi ini algılar ve yava bir a ba lantısında bile di er Internet trafi ini rahatsız etmez.

Güncelle tirme durumunu denetleme

Son güncelle tirme tarih ve saatini görüntüleyin.

Otomatik güncelle tirmeler açık oldu unda, Internet'e ba lı oldu unuzda ürün en son güncelle tirmeleri otomatik olarak alır.

Elinizde en yeni güncelle tirmelerin bulundu undan emin olmak için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Otomatik güncelle tirmeler** > **Kar ıdan yüklemeler**'i seçin.
4. **imdi denetle**'yi tıklatın.
   Ürün Internet'e ba lanır ve en son güncelle tirmeleri denetler. Koruma güncel de ilse, en yeni güncelle tirmeleri alır.

   Not: Internet'e ba lanmak için modem kullanıyorsanız veya ISDN ba lantınız varsa, güncelle tirmeleri denetleyebilmek için ba lantının etkin olması gerekir.

Internet ba lantı ayarlarımı de i tirme

Genelde varsayılan ayarların de i tirilmesi gerekmez, ancak güncelle tirmeleri otomatik olarak alabilmeniz için sunucunun Internet'e ba lanma biçimini yapılandırabilirsiniz.

Internet ba lantı ayarlarınızı de i tirmek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Otomatik güncelle tirmeler** > **Ba lantı**'yı seçin.
4. **Internet ba lantısı** listesinde, bilgisayarınızın Internet'e nasıl ba landı ını seçin.
   - Kalıcı bir a ba lantınız varsa **Her zaman ba lı varsay** seçene ini belirleyin.

     Not: Bilgisayarınızın kalıcı bir a ba lantısı yoksa ve istendi inde ba lanmak üzere ayarlanmı sa, **Her zaman ba lı varsay** seçene ini belirlemek birden fazla çevirmeli ba lantıya neden olabilir.
   - Yalnızca ürün tarafından etkin bir a ba lantısı algılandı ında güncelle tirmeleri almak için **Ba lantıyı algıla** seçene ini belirleyin.
   - Yalnızca ürün tarafından ba ka a trafi i algılandı ında güncelle tirmeleri almak için **Trafi i algıla** seçene ini belirleyin.

     pucu: Etkin a ba lantısı olmasa da **Ba lantıyı algıla** ayarının etkin bir a ba lantısı algılamasına neden olan sıra dı ı bir donanım yapılandırmanız varsa, bunun yerine **Trafi i algıla**'yı seçin.
5. **HTTP proxy** listesinde, bilgisayarınızın Internet'e ba lanmak için *proxy sunucu* kullanıp kullanmadı ını belirleyin.

- Bilgisayarınız Internet'e do rudan ba lanıyorsa, **HTTP proxy yok**'u seçin.
- **HTTP proxy'yi elle yapılandır** ö esini seçerek *HTTP proxy* ayarlarını yapılandırın.
- Web tarayıcınızda yapılandırdı ınız *HTTP proxy* ayarlarını kullanmak için **Tarayıcımın HTTP proxy'sini kullan** seçene ini belirleyin.

Gerçek Zamanlı Koruma A ı'nın durumunu denetleme

Ürünün birçok özelli inin düzgün çalı ması için Gerçek Zamanlı Koruma A ı'na ba lantı gerekir.

A sorunları varsa veya güvenlik duvarınız Gerçek Zamanlı Koruma A ı trafi ini engelliyorsa, durum 'ba lı de il' olarak görünür. Gerçek Zamanlı Koruma A ı'na eri im gerektiren herhangi bir ürün özelli i yüklü de ilse, durum 'kullanılmıyor' olarak görünür.

Durumu denetlemek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Otomatik güncelle tirmeler** > **Ba lantı**'yı seçin.

Gerçek Zamanlı Koruma A ı altında, Gerçek Zamanlı Koruma A ı'nın geçerli durumunu görebilirsiniz.

Ürününün neler yaptı ını görme

Ürünün bilgisayarınızda gerçekle tirdi i eylemleri **Bildirimler** sayfasından görebilirsiniz.

Ürün bir eylem gerçekle tirdi inde, örne in bir virüs bulup engelledi inde bir bildirim görüntüler. Bazı bildirimler, örne in kullanılabilir yeni hizmetler konusunda bilgilendirilmeniz için servis sa layıcınız tarafından da gönderilebilir.

Bildirim geçmi ini görüntüle

Görüntülenmi olan bildirimleri, bildirim geçmi inde görebilirsiniz

Bildirim geçmi ini görüntülemek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Di er** > **Bildirimler**'i seçin.
4. **Bildirim geçmi ini göster**'i tıklatın.
   Bildirim geçmi i listesi açılır.

Bildirim ayarlarını de i tirme

Ürünün hangi bildirim türlerini görüntülemesini istedi inizi seçebilirsiniz.

Bildirim ayarlarını de i tirmek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Di er** > **Bildirimler**'i seçin.

4. Program iletilerini etkinle tirmek veya devre dı ı bırakmak için **Program iletilerine izin ver**'i seçin veya seçimini kaldırın.

   Bu ayar etkinle tirildi inde, ürün, yüklü programların bildirimlerini görüntüler.
5. Tanıtım iletilerini etkinle tirmek veya devre dı ı bırakmak için **Tanıtım iletilerine izin ver**'i seçin veya seçimini kaldırın.
6. **Tamam**'ı tıklatın.

Gerçek Zamanlı Koruma A ı

Bu belgede, F-Secure Corporation tarafından sa lanan ve temiz uygulamaları ve web sitelerini tanımlamanın yanı sıra kötü amaçlı yazılımlara ve web sitesi yararlanmalarına kar ı koruma sa layan bir çevrimiçi hizmet olan Gerçek Zamanlı Koruma A ı açıklanır.

Gerçek Zamanlı Koruma A ı nedir?

Gerçek Zamanlı Koruma A ı, Internet tabanlı en son tehditlere hızlı yanıt verilebilmesini sa layan bir çevrimiçi hizmettir.

Gerçek Zamanlı Koruma A ı katılımcısı olarak yeni ortaya çıkan tehditlere kar ı korumayı güçlendirmemize yardımcı olabilirsiniz. Gerçek Zamanlı Koruma A ı, belli ba lı bilinmeyen, kötü amaçlı veya üpheli uygulamaların ve bu uygulamaların aygıtınızda yaptıklarının istatistiklerini toplar. Bu bilgiler anonimdir ve veri analiziyle birle tirilmek üzere F-Secure Corporation'a gönderilir. Analiz edilen bilgileri, en son tehditlere ve kötü amaçlı yazılımlara kar ı aygıtınızdaki güvenli i artırmak için kullanırız.

Gerçek Zamanlı Koruma A ı nasıl çalı ıyor?

Gerçek Zamanlı Koruma A ı katılımcısı olarak, bilinmeyen uygulamalar ve web siteleri ile web sitelerindeki kötü amaçlı uygulamalar ve güvenlik açıkları hakkında bilgi sa layabilirsiniz. Gerçek Zamanlı Koruma A ı web'deki etkinli inizi izlemez veya zaten analiz edilmi olan web siteleriyle ve bilgisayarınıza yüklü temiz uygulamalarla ilgili bilgi toplamaz.

Bu verilere katkıda bulunmak istemiyorsanız, Gerçek Zamanlı Koruma A ı yüklü uygulamalar veya ziyaret edilen web siteleriyle ilgili bilgi toplamaz. Ancak ürün, uygulamaların, web sitelerinin, iletilerin ve di er nesnelerin geçmi i açısından F-Secure sunucularını sorgulamak zorundadır. Sorgulama ifreli bir sa lama toplamı kullanılarak yapıldı ından sorgulanan nesnenin kendisi F-Secure'a gönderilmez. Kullanıcılara ili kin verileri izlemeyiz; yalnızca dosyanın veya web sitesinin isabet sayacı arttırılır.

Gerçek Zamanlı Koruma A ı ile ilgili a trafi i tümüyle durdurulamaz, çünkü ürün tarafından sa lanan korumanın ayrılmaz bir parçasıdır.

Gerçek Zamanlı Koruma A ı'nın faydaları

Gerçek Zamanlı Koruma A ı ile en son tehditlere kar ı daha hızlı ve daha do ru korumaya sahip olacak, kötü amaçlı olmayan üpheli uygulamalar için gereksiz uyarılar almayacaksınız.

Gerçek Zamanlı Koruma A ı katılımcısı olarak yeni ve algılanmamı kötü amaçlı yazılımları bulmamıza ve virüs tanımı veritabanımızdan hatalı pozitif sonuçları kaldırmamıza yardımcı olabilirsiniz.

Gerçek Zamanlı Koruma A ı'ndaki tüm katılımcılar birbirine yardım eder. Gerçek Zamanlı Koruma A ı aygıtınızda üpheli bir uygulama buldu unda, aynı uygulamanın daha önce ba ka aygıtlarda bulundu unda elde edilen çözümleme sonuçlarından yararlanabilirsiniz. Gerçek Zamanlı Koruma A ı, aygıtınızın genel performansını artırır; çünkü yüklü güvenlik ürününün Gerçek Zamanlı Koruma A ı tarafından daha önce çözümlenmi ve temiz oldu u belirlenmi uygulamaları yeniden taraması gerekmez. Benzer ekilde, kötü amaçlı web siteleri ve istenmeyen toplu iletiler ile ilgili bilgiler de Gerçek Zamanlı Koruma A ı aracılı ıyla payla ılır; böylece, web sitesinden yararlanma giri imlerine ve istenmeyen posta iletilerine kar ı daha do ru bir koruma sa lanabilir.

Gerçek Zamanlı Koruma A ı'na ne kadar çok insan katıkıda bulunursa, tek tek katılımcılar da o oranda daha iyi korunur.

Hangi verilere katkıda bulunursunuz?

Gerçek Zamanlı Koruma A ı katılımcısı olarak aygıtınızdaki uygulamalar ve ziyaret etti iniz web siteleri ile ilgili bilgi sa larsınız; böylece Gerçek Zamanlı Koruma A ı en yeni kötü amaçlı uygulamalar ve üpheli web sitelerine kar ı korunmanızı sa layabilir.

Dosya yorumunu çözümleme

Gerçek Zamanlı Koruma A yalnızca bilinen bir yorum bulunmayan uygulamalar ve üpheli ya da kötü amaçlı oldu u bilinen dosyalar ile ilgili bilgileri toplar.

Gerçek Zamanlı Koruma A ı yalnızca ta ınabilir yürütülebilir dosyalar (Windows platformundaki .cpl, .exe, .dll, .ocx, .sys, .scr ve .drv dosya uzantılı Ta ınabilir Yürütülebilir dosyalar gibi) ile ilgili bilgileri toplar.

Toplanan bilgiler unları içerir:

- uygulamanın aygıtınızda bulundu u dosya yolu,
- dosyanın boyutu ve olu turulma ya da de i tirilme tarihi,
- dosya öznitelikleri ve ayrıcalıklar,
- dosya imzası bilgileri,
- dosyanın geçerli sürümü ve dosyayı olu turan irket,
- dosyanın kayna ı veya kar ıdan yükleme URL'si,
- taranan dosyaların F-Secure DeepGuard ve virüsten koruma çözümlemesi sonuçlarını
- di er benzer bilgiler.

Gerçek Zamanlı Koruma A ı, etkilenmi oldukları belirlenmedikçe ki isel belgelerinizle ilgili herhangi bir bilgi toplamaz. Kötü amaçlı dosya türleri için, etkilenmenin adı ve dosyanın temizleme durumu ile ilgili bilgiler toplanır.

Gerçek Zamanlı Koruma A ı aracılı ıyla, çözümlenmek üzere üpheli yazılımları da gönderebilirsiniz. Gönderebilece iniz uygulamalar yalnızca Ta ınabilir Yürütülebilir dosyalar olabilir. Gerçek Zamanlı Koruma A ı hiçbir zaman ki isel belgelerinizle ilgili herhangi bir bilgi toplamaz ve bu tür dosyalar hiçbir zaman çözümlenmek üzere otomatik olarak kar ıya yüklenmez.

Dosyaları çözümlenmek üzere gönderme

Gerçek Zamanlı Koruma A ı ile üpheli uygulamaları analiz için göndermeniz de mümkündür.

 üpheli uygulamaları, ürün sizden bunu istedi i zaman gönderebilirsiniz. Yalnızca Ta ınabilir Yürütülebilir dosyaları gönderebilirsiniz. Gerçek Zamanlı Koruma A ı hiçbir zaman ki isel belgelerinizi yüklemez.

Web sitesi yorumunu çözümleme

Gerçek Zamanlı Koruma A ı, web etkinli inizi izlemez veya daha önce çözümlenmi olan web siteleri ile ilgili bilgi toplamaz. Web'de gezindi iniz sırada ziyaret etti iniz web sitelerinin güvenli oldu undan emin olmanızı sa lar. Bir web sitesini ziyaret etti inizde, Gerçek Zamanlı Koruma A ı bu sitenin güvenilir olup olmadı ını denetler ve site üpheli ya da zararlı olarak derecelendirilmi se size bildirir.

Ziyaret etti iniz web sitesinde kötü amaçlı veya üpheli içerik varsa veya bilinmeyen bir yararlanma kodu kullanılıyorsa, Gerçek Zamanlı Koruma A ı, web sayfası içeri inin çözümlenebilmesi için bu sitenin tüm URL'sini toplar.

Henüz derecelendirilmemi bir siteyi ziyaret ederseniz, Gerçek Zamanlı Koruma A ı, sitenin çözümlenebilmesi ve derecelendirilebilmesi için etki alanı ve alt etki alanı adlarının yanı sıra bazı durumlarda ziyaret edilen sayfanın yolunu da toplar. Gizlili inizi korumak için, ki isel olarak tanımlanmanıza olanak verebilecek ekilde sizinle ba lantılı olan bilgiler içerebilecek tüm URL parametreleri kaldırılır.

Not: Gerçek Zamanlı Koruma A ı özel a lardaki web sayfalarını derecelendirmez veya çözümlemez; bu nedenle de özel IP a ı adreslerinden (örne in, kurumsal intranetlerden) hiçbir bilgi toplamaz.

Sistem bilgisini çözümleme

Gerçek Zamanlı Koruma A ı, hizmeti izleyebilmemiz ve geli tirebilmemiz için i letim sisteminizin adı ve sürümü, Internet ba lantısı ve Gerçek Zamanlı Koruma A ı kullanım istatistikleri (örne in, web sitesi yorumunun sorgulanma sayısı ve sorgunun bir sonuç döndürmesi için geçen ortalama süre) ile ilgili bilgi toplar.

Gizlili iniz nasıl korunuyor?

Bu bilgileri güvenli ekilde aktarır ve verilerin içerebilece i ki isel bilgileri otomatik olarak kaldırırız.

Gerçek Zamanlı Koruma A ı, kimlik belirleyici verileri F-Secure'a göndermeden önce kaldırır ve aktarım sırasında toplanan tüm bilgileri ifreleyerek yetkisiz eri imden korunmasını sa lar. Toplanan bilgiler tek tek i lenmez; di er Gerçek Zamanlı Koruma A ı katılımcılarından alınan bilgilerle birlikte gruplandırılır. Tüm veriler istatistiksel ve anonim olarak analiz edilir; bu, hiçbir verinin hiçbir ekilde size ba lanmayaca ı anlamına gelir.

Toplanan veriler, sizi ki isel olarak tanımlayabilecek herhangi bir bilgi içermez. Gerçek Zamanlı Koruma A ı özel IP adresini ya da e-posta adresleri, kullanıcı adları ve parolalar gibi di er özel bilgileri toplamaz. Ki isel olarak tanımlanmanıza yol açabilecek tüm verileri kaldırmaya çalı mamıza kar ın, toplanan bilgilerde bu tür veriler kalabilir. Bu gibi durumlarda, istenmeden toplanan verileri sizi ki isel olarak tanımlamak için kullanmayaca ız.

Toplanan bilgilerin aktarılması, depolanması ve i lenmesi sırasında katı güvenlik önlemleri ve fiziksel, yönetimsel ve teknik korumalar uygularız. Bu bilgiler, kendi ofislerimizde veya alt yüklenicilerimizin ofislerinde bulunan güvenli konumlarda ve bizim denetimimizdeki sunucularda depolanır. Toplanan bilgilere yalnızca yetkili personel eri im sa layabilir.

F-Secure toplanan verileri ba lı irketleri, alt yüklenicileri, da ıtımcıları ve ortaklarıyla payla abilir; ancak bunu her zaman, ki isel olarak tanımlanamayacak anonim bir biçimde yapar.

Gerçek Zamanlı Koruma A ı katılımcısı olma

Kötü amaçlı programlar ve web siteleri ile ilgili bilgilere katkıda bulunarak Gerçek Zamanlı Koruma A ı korumasının geli tirilmesine yardım edebilirsiniz.

Yükleme sırasında Gerçek Zamanlı Koruma A ı'na katılmayı seçebilirsiniz. Varsayılan yükleme ayarlarıyla Gerçek Zamanlı Koruma A ı verilerine katkıda bulunursunuz. Bu ayarları daha sonra ürünün içinde de i tirebilirsiniz.

Gerçek Zamanlı Koruma A ı ayarlarını de i tirmek için a a ıdaki yönergeleri izleyin:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Di er** > **Gizlilik**'i seçin.
4. Gerçek Zamanlı Koruma A ı katılımcısı olmak için katılım onay kutusunu i aretleyin.

Gerçek Zamanlı Koruma A ı ile ilgili sorular

Gerçek Zamanlı Koruma A ı ile ilgili sorular için ileti im bilgileri.

Gerçek Zamanlı Koruma A ı ile ilgili ba ka sorularınız varsa lütfen u adrese ba vurun:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlandiya

http://www.f-secure.com/en/web/home_global/support/contact

Bu ilkenin en son sürümü her zaman web sitemizden edinilebilir.

Aboneli imin geçerli oldu unu nasıl bilebilirim

Abonelik türünüz ve durumunuz **Abonelik durumu** sayfasında gösterilir.

Aboneli inizin süresi dolmak üzereyken veya dolmu sa, kar ılık gelen LaunchPad simgesindeki programın toplam koruma durumu de i ir.

Aboneli inizin geçerlili ini denetlemek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Aboneliklerimi görüntüle** seçene ini belirtin.
3. Yüklü programlar için aboneliklerinizle ilgili bilgileri görüntülemek için **Abonelik durumu**'nu seçin.
4. Yüklenebilecek programları görmek için **Yükleme durumu**'nu seçin.

Abonelik durumunuz ve süre sonunuz da programın **statistikler** sayfasında gösterilir. Aboneli inizin süresi dolmu sa, güncelle tirmeleri almaya ve ürünü kullanmaya devam edebilmek için aboneli inizi yenilemeniz gerekir.

Not: Aboneli inizin süresi doldu unda, sistem tepsinizdeki ürün durumu simgesi yanıp söner.

Eylem merkezi

Eylem merkezi ilgilenmeniz gereken önemli bildirimleri size gösterir.

Aboneli inizin süresi dolduysa veya dolmak üzereyse eylem merkezi sizi bu durumdan haberdar eder. Eylem merkezi mesajının arka plan rengi ve içeri i abonelik türünüze ve durumunuza ba lıdır:

- Abonelik süreniz dolmak üzereyse ve ücretsiz abonelikler mevcutsa mesajın arka plan rengi beyazdır ve bir **Etkinle tir** dü mesi görüntülenir.
- Abonelik süreniz dolmak üzereyse ancak ücretsiz abonelikler mevcut de ilse mesajın arka plan rengi sarıdır ve ekranda **Satın al** ve **Anahtarı gir** dü meleri görüntülenir. Yeni almı oldu unuz bir abonelik varsa **Anahtarı gir** dü mesini tıklatarak size sa lanmı olan anahtarı girebilir ve aboneli inizi etkinle tirebilirsiniz.
- Abonelik süreniz dolduysa ve ücretsiz abonelikler mevcutsa mesajın arka plan rengi kırmızıdır ve bir **Etkinle tir** dü mesi görüntülenir.
- Abonelik süreniz dolduysa ancak ücretsiz abonelikler mevcut de ilse mesajın arka plan rengi kırmızıdır ve ekranda **Satın al** ve **Anahtarı gir** dü meleri görüntülenir. Yeni almı oldu unuz bir abonelik varsa **Anahtarı gir** dü mesini tıklatarak size sa lanmı olan anahtarı girebilir ve aboneli inizi etkinle tirebilirsiniz.

Not: Eylem merkezindeki **Bildirim geçmi ini görüntüle** ba lantısı ürün bildirim mesajlarını içeren bir liste görüntüler, önceki eylem merkezi bildirimleri burada görüntülenmez.

Aboneli i etkinle tir

Bir ürün için yeni bir abonelik anahtarınız veya kampanya kodunuz varsa, bunu etkinle tirmeniz gerekir.

Aboneli i etkinle tirmek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.
   Açılır menü görüntülenir.
2. **Aboneliklerimi görüntüle** seçene ini belirtin.
3. A a ıdakilerden birini seçin:
   - **Aboneli i etkinle tir**'i tıklatın.
   - **Kampanya kodunu etkinle tir**'i tıklatın.
4. Açılan ileti im kutusunda, yeni abonelik anahtarınızı veya kampanya kodunuzu girin ve **Tamam**'ı tıklatın.

   pucu: Abonelik anahtarınızı e-posta yoluyla aldıysanız, anahtarı e-posta iletisinden kopyalayıp bu alana yapı tırabilirsiniz.

Yeni abonelik anahtarını girdikten sonra, yeni abonelik geçerlilik tarihi **Abonelik durumu** sayfasında gösterilir.

Bölüm

3

Giri

Konular:

- *Genel koruma durumunuzu görüntüleme*
- *Ürün istatistiklerini görüntüleme*
- *Ürün güncelle tirmelerini i leme*
- *Virüsler ve di er kötü amaçlı yazılımlar nedir*

Bu ürün, bilgisayarınızı virüslere ve di er yazılım uygulamalarına kar ı korur.

Ürün, dosyaları tarar, uygulamaları analiz eder ve otomatik olarak güncelle tirme yapar. Sizin hiçbir ey yapmanız gerekmez.

Genel koruma durumunuzu görüntüleme

Durum sayfası, yüklü ürün özelliklerine ve bu ürünlerin geçerli durumuna hızlı bir genel bakı sunar.

Durum sayfasını açmak için:

Ana sayfada **Durum**'u tıklatın.

Durum sayfası açılır.

Simgeler, programın durumunu ve güvenlik özelliklerini gösterir.

Durum simgesi	Durum adı	Açıklama
	Tamam	Bilgisayarınız korunuyor. Özellik etkinle tirildi ve düzgün çalı ıyor.
	Bilgi	Ürün, özelli in özel durumu hakkında sizi bilgilendirir. Örne in, özellik güncelle tiriliyor.
	Uyarı	Bilgisayarınız tam olarak korunmuyor. Örne in, ürün uzun süredir güncelle tirme almadı ya da bir özelli in durumuyla ilgilenilmesi gerekiyor.
	Hata	Bilgisayarınız korunmuyor. Örne in, aboneli inizin süresi doldu ya da önemli bir özellik kapalı.
	Kapalı	Kritik olmayan bir özellik devre dı ı bırakıldı.

Ürün istatistiklerini görüntüleme

Ürünün yüklenmesinden bu yana yaptı ı i lemleri **statistikler** sayfasında görebilirsiniz.

statistikler sayfasını açmak için:

Ana sayfada **statistikler**'i tıklatın.

statistikler sayfası açılır.

- **Son ba arılı güncelle tirme denetimi**, son güncelle tirme saatini gösterir.
- **Virüs ve casus yazılım taraması**, ürünün yüklendikten sonra kaç dosya taradı ını ve temizledi ini gösterir.
- **Uygulamalar**, DeepGuard'ın yüklemeden bu yana kaç programa izin verdi ini veya engelledi ini gösterir.
- **Güvenlik duvarı ba lantıları**, yüklemeden itibaren izin verilen ve engellenen ba lantıların sayısını gösterir.

- **stenmeyen e-posta ve kimlik avı filtreleme**, ürünün geçerli e-posta iletileri ve istenmeyen e-posta iletileri olarak kaç tane e-posta iletisi algıladı ını gösterir.

Ürün güncelle tirmelerini i leme

Ürün, korumayı otomatik olarak güncel tutar.

Veritabanı sürümlerini görüntüleme

Veritabanı güncelle tirmeleri sayfasından en son güncelle tirme zamanlarını ve sürüm numaralarını görebilirsiniz.

Veritabanı güncelle tirmeleri sayfasını açmak için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar** > **Veritabanı sürümleri** ö elerini seçin.

Veritabanı sürümleri sayfasında, virüs ve casus yazılım tanımları, DeepGuard ve istenmeyen e-posta ve kimlik avı filtrelemenin güncelle tirildi i en son tarih ve sürüm numaraları görüntülenir.

Cep telefonu geni bant ayarlarını de i tir

Cep telefonu geni bant ba lantı kullanırken güvenlik güncelle tirmelerini kar ıdan yüklemek için seçin.

Not: Bu özellik yalnızca Microsoft Windows 7'de kullanılabilir.

Varsayılan olarak, asıl operatörünüzün a ındayken güvenlik güncelle tirmeleri her zaman kar ıdan yüklenir. Ancak ba ka bir operatörün a ını kullanıyorsanız güncelle tirmeler askıya alınır. Bunun nedeni, örne in farklı ülkelerde ba lantı ücretlerinin operatörlere göre de i ebilmesidir. Ziyaretiniz sırasında bant geni li inden ve maliyetlerden tasarruf etmek için bu ayarı de i tirmeden kullanmak isteyebilirsiniz.

Not: Bu ayar yalnızca cep telefonu geni bant ba lantılar için geçerlidir. Bilgisayarın bir sabit ya da kablosuz a a ba lı oldu u sırada ürün otomatik olarak güncelle tirilir.

Bu ayarı de i tirmek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar** > **Mobil geni bant** > **Güvenlik güncelle tirmelerini kar ıdan yükle** ö elerini seçin.
3. Cep telefonu ba lantıları için tercih edilen güncelle tirme seçene ini belirleyin:
   - **Yalnızca ev operatörümün a ında**

     Güncelle tirmeler her zaman asıl operatörünüzün a ındayken kar ıdan yüklenir. Ba ka bir operatörün a ını kullanıyorsanız güncelle tirmeler askıya alınır. Öngörülen maliyetleri göze alarak güvenlik ürününüzü güncel tutmak üzere bu seçene i belirlemeniz önerilir.
   - **Hiçbir zaman**

     Mobil geni bant kullandı ınızda güncelle tirmeler kar ıdan yüklenmez.
   - **Her zaman**

     Hangi a ı kullanıyor olursanız olun güncelle tirmeler her zaman kar ıdan yüklenir. Maliyetler ne olursa olsun bilgisayarınızın güvenli inin her zaman güncel olmasını istiyorsanız bu seçene i belirleyin.

4. Ev operatörünüzün a ından her çıkı ınızda ayrıca karar vermek istiyorsanız, **Ev operatörümün a ından her çıkı ımda bana sor** seçene ini belirleyin.

Askıya alınmı güvenlik güncelle tirmeleri

Asıl operatörünüzün a ı dı ında bir cep telefonu geni bant ba lantı kullanırken güvenlik güncelle tirmeleri askıya alınabilir.

Bu durumda, ekranınızın sa alt kö esinde **Askıya Alındı** bildirim duyurusunu görebilirsiniz. Ba lantı fiyatları operatörlere göre de i ebilece inden (örne in farklı ülkelerde) güncelle tirmeler askıya alınır. Ziyaretiniz sırasında bant geni li inin yanı sıra maliyet tasarrufu da yapmak istiyorsanız, bu ayarı de i tirmeden korumayı dü ünebilirsiniz. Ancak yine de ayarları de i tirmek istiyorsanız, **De i tir** ba lantısını tıklatın.

Not:

Bu özellik yalnızca Microsoft Windows 7'de kullanılabilir.

Virüsler ve di er kötü amaçlı yazılımlar nedir

Kötü amaçlı yazılımlar bilgisayarınıza zarar vermek, bilginiz olmadan bilgisayarınızı yasa dı ı amaçlarla kullanmak veya bilgisayarınızdan bilgi çalmak için özel olarak tasarlanmı programlardır.

Kötü amaçlı yazılımlar unları yapabilir:

- Web tarayıcınızın denetimini ele geçirir,
- arama denemelerinizi yeniden yönlendirir,
- istenmeyen reklamlar gösterir,
- ziyaret etti iniz Web sitelerinin kaydını tutar,
- banka bilgileri gibi ki isel bilgilerinizi çalar,
- bilgisayarınızı kullanarak istenmeyen posta gönderir ve
- bilgisayarınızı kullanarak ba ka bilgisayarlara saldırır.

Kötü amaçlı yazılımlar bilgisayarınızın yava lamasına ve kararsız olmasına da neden olabilir Bilgisayarınız aniden çok yava larsa ve sık sık kilitlenirse *kötü amaçlı yazılımlar* oldu undan üphelenebilirsiniz.

Virüsler

Virüs, genellikle kendini dosyalara ekleyerek sürekli olarak ço altabilen programdır; bilgisayarınıza zarar verebilecek bir ekilde di er dosyaların içeri ini de i tirebilir.

Virüs normalde bilginiz olmadan bilgisayarınıza yüklenen bir programdır. Virüs bula tıktan sonra kendisini ço altmaya çalı ır. Virüs unları yapabilir:

- bilgisayarınızın sistem kaynaklarının bir bölümünü kullanır,
- bilgisayarınızdaki dosyaları de i tirebilir veya dosyalara zarar verebilir,
- bilgisayarınızı kullanarak ba ka bilgisayarları etkilemeye çalı abilir,
- bilgisayarınızın yasa dı ı amaçlarla kullanılmasına neden olabilir.

Casus yazılımlar

Casus yazılımlar ki isel bilgilerinizi toplayan programlardır.

Casus yazılımlar unun gibi ki isel bilgileri toplar:

- Gözattı ınız Internet siteleri,
- bilgisayarınızdaki e-posta adresleri,
- parolalar veya

- kredi kartı numaraları.

Casus yazılımlar neredeyse her zaman açıkça izniniz olmadan kendilerini yükler. Casus yazılımlar yararlı bir programla birlikte ya da yanıltıcı bir açılır pencerede bir seçene i tıklatmanızı sa layarak yüklenebilir.

Kendini gizleyen yazılımlar

Kendini gizleyen yazılımlar, di er *kötü amaçlı yazılımlar*'ı bulmayı zorla tırır.

Kendini gizleyen yazılımlar, dosyaları ve i lemleri gizler. Bunu genel olarak bilgisayarınızdaki kötü amaçlı etkinli i gizlemek için yaparlar. Kendini gizleyen bir yazılım *kötü amaçlı yazılımlar*'ı gizliyorsa, bilgisayarınızda kötü amaçlı yazılım oldu unu kolay bir ekilde anlayamazsınız.

Bu üründe, özellikle kendini gizleyen yazılımlar için tarama yaparak *kötü amaçlı yazılımlar*'ın kolayca gizlenememesini sa layan bir kendini gizleyen yazılım tarayıcısı vardır.

Riskli yazılımlar

Riskli yazılımlar bilgisayarınıza zarar vermek amacıyla özel olarak tasarlanmamı lardır, ancak yanlı kullanılırlarsa bilgisayarınıza zarar verebilir.

Riskli yazılımların mutlaka kötü amaçlı yazılım olması gerekmez. Riskli yazılım programları bazı kullanı lı, ancak zararlı olabilecek i levler gerçekle tirir.

Riskli yazılım programlarına örnek olarak unlar gösterilebilir:

- IRC (Internet relay chat) gibi anlık ileti programları,
- bir bilgisayardan di erine Internet üzerinden dosya aktarmaya yönelik programlar,
- veya Internet telefonu programları (VoIP, *Internet Üzerinden Ses Protokolü*).
- VNC gibi Uzaktan Eri im Yazılımları,
- ki ileri korkutarak veya oyuna getirerek sahte güvenlik yazılımları almaya yönlendiren korkutma yazılımları veya
- CD denetimlerini veya kopyalama korumalarını atlamak için tasarlanan yazılımlar.

Programı açık olarak yüklediyseniz ve do ru ekilde kurduysanız, zararlı olma olasılı ı daha azdır.

Riskli yazılım bilginiz dı ında yüklendiyse, büyük olasılıkla kötü amaçlı olarak yüklenmi tir ve kaldırılması gerekir.

Bölüm

4

Kötü amaçlı yazılımlara kar ı bilgisayarı koruma

Konular:

- *Bilgisayarımı nasıl tarayabilirim*
- *Dosyalar nasıl taramanın dı ında bırakılır*
- *Karantina nasıl kullanılır*
- *DeepGuard nedir*

Virüs ve casus yazılım taraması bilgisayarınızı ki isel bilgileri çalan, bilgisayarınıza zarar veren veya yasa dı ı amaçlarla kullanan programlara kar ı korur.

Varsayılan olarak, tüm kötü amaçlı yazılım türleri hiçbir zarar vermemeleri için bulunur bulunmaz i lenir.

Virüs ve casus yazılım taraması varsayılan olarak yerel sabit sürücülerinizi, çıkarılabilir ortamlarınızı (ta ınabilir sürücüler veya CD'ler gibi) ve kar ıdan yüklenen içeri i otomatik olarak tarar. E-postalarınızı da otomatik olarak taranacak ekilde ayarlayabilirsiniz.

Virüs ve casus yazılım taraması ayrıca bilgisayarınızda *kötü amaçlı yazılım* göstergesi olabilecek de i iklikleri de izler. Sistem ayarlarında tehlikeli olabilecek de i iklikler veya önemli sistem i lemlerini de i tirme denemeleri bulunursa, *kötü amaçlı yazılım* söz konusu olabilece inden DeepGuard bu programların çalı masını durdurur.

Bilgisayarımı nasıl tarayabilirim

Virüs ve casus yazılım taraması açıkken, bilgisayarınızı zararlı dosyalara kar ı otomatik olarak tarar. Aynı zamanda dosyaları elle tarayabilir ve zamanlanan taramalar ayarlayabilirsiniz.

Virüs ve casus yazılım taramasını her zaman açık tutmanızı öneririz. Bilgisayarınızda hiç zararlı dosya olmadı ından emin olmak istedi inizde ya da gerçek zamanlı taramanın dı ında bıraktı ınız dosyaları taramak isterseniz, dosyalarınızı elle tarayın.

Virüs ve casus yazılım taraması zamanlanan bir tarama ayarlayarak, zararlı dosyaları belirlenen zamanlarda bilgisayarınızdan kaldırır.

Dosyaları otomatik olarak tarama

Gerçek zamanlı tarama, eri ilen tüm dosyaları tarayıp *kötü amaçlı yazılımlar* içeren dosyalara eri imi engelleyerek bilgisayarınızı korur.

Bilgisayarınız bir dosyaya eri meye çalı tı ında, Gerçek zamanlı tarama bilgisayarınızın bu dosyaya eri mesine izin vermeden önce dosyayı kötü amaçlı yazılımlara kar ı tarar. Gerçek zamanlı tarama herhangi bir zararlı içerik bulursa, zarar verememesi için dosyayı karantinaya alır.

Gerçek zamanlı tarama bilgisayarımın performansını etkiler mi?

Normalde, çok kısa sürdü ü ve sistem kaynaklarını çok az kullandı ı için tarama i lemini fark etmezsiniz. Gerçek zamanlı tarama için kullanılan süre ve sistem kaynakları, dosyanın içeri ine, konumuna ve türüne ba lı olarak de i ebilir.

Taranması daha fazla zaman alan dosyalar:

- CD, DVD ve ta ınabilir USB sürücüleri gibi çıkarılabilir sürücülerdeki dosyalar.
- Sıkı tırılmı dosyalar, örne in: *.zip* dosyaları.

  Not: Sıkı tırılmı dosyalar varsayılan olarak taranmaz.

Gerçek zamanlı tarama u durumlarda bilgisayarınızı yava latabilir:

- Sistem gereksinimlerini kar ılamayan bir bilgisayarınız var ya da
- aynı anda birçok dosyaya eri iyorsunuz; örne in, taranması gereken birçok dosya içeren bir dizini açıyorsunuz.

Gerçek zamanlı taramayı açma veya kapatma

Kötü amaçlı yazılımları bilgisayarınıza zarar vermeden önce durdurmak için gerçek zamanlı taramayı açık tutun.

Gerçek zamanlı taramayı açmak veya kapatmak için:

1. Ana sayfada **Durum**'u tıklatın.
2. **Bu sayfadaki ayarları de i tir**'i tıklatın.

   Not: Güvenlik özelliklerini kapatmak için yönetici haklarınızın olması gerekir.

3. **Virüs ve casus yazılım taraması**'nı açın veya kapatın.
4. **Kapat**'ı tıklatın.

Zararlı dosyaları otomatik olarak i leme

Gerçek zamanlı tarama, size hiçbir ey sormadan zararlı dosyaları otomatik olarak i leyebilir.

Gerçek zamanlı taramanın zararlı dosyaları otomatik olarak i lemesine izin vermek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i** > **Virüs ve casus yazılım taraması** ö elerini seçin.
3. **Zararlı dosyaları otomatik olarak i le** ö esini seçin.

Zararlı dosyaları otomatik olarak i lemeyi seçmezseniz, gerçek zamanlı tarama zararlı bir dosya bulundu unda dosyayla ne yapmak istedi inizi sorar.

Casus yazılımları i leme

Virüs ve casus yazılım taraması, ba latılmaya çalı tı ında casus yazılımı hemen engeller.

Bir casus yazılım uygulaması ba latılmadan önce, ürün bu uygulamayı engeller ve uygulamayla ne yapmak istedi inize karar vermenize izin verir.

Bir casus yazılım bulundu unda a a ıdaki eylemlerden birini seçin:

Gerçekle tirilecek eylem	Casus yazılım için hangi eylemler gerçekle tirilir
Otomatik i le	Bulunan casus yazılıma göre alınacak en iyi önleme ürünün karar vermesine izin verin.
Casus yazılımı karantinaya al	Casus yazılımı, bilgisayarınıza zarar veremeyece i karantinaya ta ıyın.
Casus yazılımı sil	Tüm casus yazılımla ilgili dosyaları bilgisayarınızdan kaldırın.
Casus yazılımı yalnızca engelle	Casus yazılıma eri imi engelleyin ancak yazılımı bilgisayarınızda bırakın.
Casus yazılımı taramanın dı ında bırak	Casus yazılımın çalı masına izin verin ve yazılımı gelecekteki taramaların dı ında bırakın.

Riskli yazılımları i leme

Virüs ve casus yazılım taraması, riskli yazılımı ba latılmaya çalı ırken hemen engeller.

Bir riskli yazılım uygulaması ba latılmadan önce, ürün uygulamayı engeller ve uygulamayla ne yapmak istedi inize karar vermenize izin verir.

Bir riskli yazılım bulundu unda a a ıdaki eylemlerden birini seçin:

Gerçekle tirilecek eylem	Riskli yazılımlar için hangi eylemler gerçekle tirilir
Riskli yazılımı yalnızca engelle	Riskli yazılıma eri imi engelleyin ancak yazılımı bilgisayarınızda bırakın.
Riskli yazılımı karantinaya al	Riskli yazılımı bilgisayarınıza zarar veremeyece i karantinaya ta ıyın.
Riskli yazılımı sil	Tüm riskli yazılımla ilgili dosyaları bilgisayarınızdan kaldırın.
Riskli yazılımı taramanın dı ında bırak	Riskli yazılımın çalı masına izin verin ve yazılımı gelecekteki taramaların dı ında bırakın.

zleme çerezlerini otomatik olarak kaldırma

zleme çerezlerini kaldırarak, web sitelerinin Internet'te ziyaret etti iniz siteleri izlemesini durdurursunuz.

zleme çerezleri, web sitelerinin ziyaret etti iniz web sitelerini kaydetmesine izin veren küçük dosyalardır. zleme çerezlerini bilgisayarınızdan kaldırmak için u yönergeleri izleyin.

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i** > **Virüs ve casus yazılım taraması** ö elerini seçin.
3. **zleme çerezlerini kaldır** ö esini seçin.
4. **Tamam**'ı tıklatın.

Dosyaları elle tarama

Örne in, bilgisayarınıza harici bir aygıt ba ladı ınızda, bu aygıtın herhangi bir kötü amaçlı yazılım içerip içermedi inden emin olmak için dosyalarınızı elle tarayabilirsiniz.

Elle taramayı ba latma

Tüm bilgisayarınızı veya belirli türde *kötü amaçlı yazılımlar*'ı ya da belirli bir konumu tarayabilirsiniz.

Belirli bir türde *kötü amaçlı yazılımlar* oldu undan üpheleniriseniz, yalnızca bu tür için tarama gerçekle tirebilirsiniz. Bilgisayarınızdaki belirli bir konumdan üpheleniyorsanız, yalnızca bu bölümü tarayabilirsiniz. Bu taramalar tüm bilgisayarın taranmasından çok daha kısa sürede tamamlanır.

Bilgisayarınızı elle taramayı ba latmak için:

1. Ana sayfada **Tara**'nın altındaki oku tıklatın.

   Tarama seçenekleri gösterilir.

2. Tarama türünü seçin.

   Elle taramanın, bilgisayarınızı virüslere ve di er zararlı uygulamalara kar ı tarama biçimini iyile tirmek için **Tarama ayarlarını de i tir**'i seçin.

3. **Taranacak ö eleri seçin**'i seçerseniz, taranacak konumu belirleyebilece iniz bir pencere açılır. **Tarama Sihirbazı** açılır.

Tarama türleri

Tüm bilgisayarınızı veya belirli türde kötü amaçlı yazılımlar'ı ya da belirli bir konumu tarayabilirsiniz.

A a ıda farklı tarama türleri listelenmi tir:

Tarama türü	Neler taranır	Bu tür ne zaman kullanılır
Virüs ve casus yazılım taraması	Bilgisayarınızın bölümlerinde virüs, casus yazılım ve riskli yazılım taraması	Bu tarama türü tam taramadan çok daha hızlıdır. Sisteminizin yalnızca yüklü program dosyaları bulunan bölümlerini tarar. Bu tarama türü hızlı bir ekilde bilgisayarınızın temiz olup olmadı ını denetlemek istiyorsanız önerilir; çünkü bilgisayarınızdaki etkin kötü amaçlı yazılımları etkili bir ekilde bulabilir ve kaldırabilir.
Tam bilgisayar taraması	Bilgisayarınızın tamamında (dahili ve harici sabit sürücüler) virüs, casus yazılım ve riskli yazılım taraması	Bilgisayarınızda kötü amaçlı yazılım veya riskli yazılım olmadı ından kesin emin olmak istedi inizde. Bu tarama türü tamamlanması en uzun süren türdür. Hızlı kötü amaçlı yazılım taraması ile sabit sürücü taramasını birle tirir. Bir kendini gizleyen yazılım tarafından gizlenebilecek ö eleri de denetler.
Taranacak ö eleri seçin	Belirli bir dosya, klasör veya sürücüde virüs, casus yazılım ve riskli yazılım taraması	Bilgisayarınızda belirli bir konumda kötü amaçlı yazılımlar olabilece inden üpheleniyorsanız; örne in, konumda e ler arası dosya payla ım a ları gibi tehlikeli olabilecek kaynaklardan kar ıdan yüklenmi ö eler varsa. Tarama süresi taradı ınız hedefin boyutuna göre de i ir. Örne in,

Tarama türü	Neler taranır	Bu tür ne zaman kullanılır
		birkaç küçük dosya içeren bir klasörü tararsanız i lem hızlı bir ekilde tamamlanır.
Kendini gizleyen yazılım taraması	üpheli bir ö enin bir güvenlik sorununa neden olabilece i önemli sistem konumları. Gizli dosyaları, klasörleri, sürücüleri veya i lemleri tarar	Bilgisayarınıza kendini gizleyen bir yazılım yüklendi inden üpheleniyorsanız. Örne in, yakın zaman önce bilgisayarınız kötü amaçlı yazılım algılandıysa ve bunun bir kendini gizleyen yazılım yüklemedi inden emin olmak istiyorsanız.

Windows Gezgini'nde tarama

Windows Gezgini'nde disklerde, klasörlerde ve dosyalarda *virüs*, *casus yazılım* ve *riskli yazılım* taraması yapabilirsiniz.

Bir diski, klasörü veya dosyayı taramak için:

1. Fare i aretçisini tarama yapmak istedi iniz disk, klasör veya dosya üzerine getirin ve sa tıklatın.
2. Sa tıklattı ınızda açılan menüden **Klasörlerde Virüs Taraması Yap** seçene ini belirleyin. (Seçenek adı, taradı ınız ö enin bir disk, klasör veya dosya olmasına ba lı olarak de i ir.)
   Tarama Sihirbazı penceresi açılır ve tarama ba lar.

Bir *virüs* veya *casus yazılım* bulunursa, **Tarama Sihirbazı** temizleme i lemlerinde size yol gösterir.

Taranacak dosyaları seçme

Elle ve zamanlanan taramalarda *virüsler* ve *casus yazılımlar* için taranmasını istedi iniz dosya türlerini seçebilirsiniz.

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar** > **Elle tarama** ö elerini seçin.
3. **Tarama seçenekleri**'nin altında a a ıdaki ayarlar arasından seçim yapın:

   Yalnızca bilinen dosya türlerini tara
   Yürütülebilir dosyalar gibi yalnızca etkilenme olasılı ı en fazla olan dosya türlerini taramak için. Bu seçene in kullanılması ayrıca taramanın hızlanmasını da sa lar. u uzantılara sahip dosyalar taranır: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` ve `.hqx`.

   Sıkı tırılmı dosyaların içini tara
   Ar iv dosyalarını ve klasörleri taramak için.

   Geli mi bulu sal yöntem kullan
   Yeni ve bilinmeyen kötü amaçlı yazılımları daha iyi bulmak için tarama sırasında tüm kullanılabilir bulu sal yöntemleri kullanmak için.

   Not: Bu seçene i belirlerseniz, tarama daha uzun sürer ve daha çok yanlı pozitif sonuç verebilir (zararsız dosyalar üpheli olarak raporlanabilir).

4. **Tamam**'ı tıklatın.

Not: Dı arıda bırakılan ö eler listesindeki dı arıda bırakılan dosyalar, burada taranmalarını seçseniz bile taranmaz.

Zararlı dosyalar bulundu unda ne yapmak gerekir

Zararlı dosyalar bulundu unda bunları nasıl i lemek istedi inizi seçin.

Elle tarama sırasında zararlı içerik bulundu unda yapılacak eylemleri seçmek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar** > **Elle tarama** ö elerini seçin.
3. **Virüs veya casus yazılım bulundu unda** ö esinde, a a ıdaki seçeneklerden birini belirleyin:

Seçenek	Açıklama
Bana sor (varsayılan)	Elle tarama sırasında bulunan her ö e için yapılacak eylemi seçebilirsiniz.
Dosyaları temizle	Ürün, elle tarama sırasında bulunan etkilenen dosyaları otomatik olarak temizlemeye çalı ır. **Not:** Ürün etkilenen dosyayı temizleyemezse (a da veya çıkarılabilir sürücülerde bulunmadı ı sürece) karantinaya alır, böylece dosya bilgisayara zarar veremez.
Dosyaları karantinaya al	Ürün, elle tarama sırasında bulunan tüm zararlı dosyaları bilgisayara zarar veremeyecekleri karantinaya ta ır.
Otomatik olarak sil	Ürün, elle tarama sırasında bulunan tüm zararlı dosyaları siler.
Yalnızca bildir	Ürün, elle tarama sırasında bulunan tüm zararlı dosyaları oldukları gibi bırakır ve tarama raporuna algılamayı kaydeder. **Not:** Gerçek zamanlı tarama etkin de ilse, bu seçene i belirledi inizde kötü amaçlı yazılımlar bilgisayara yine de zarar verebilir.

Not: Zamanlanan tarama sırasında zararlı dosyalar bulundu unda, bu dosyalar otomatik olarak temizlenir.

Tarama zamanlama

Bilgisayarınızı, virüsleri ve di er zararlı uygulamaları bilgisayarı kullanmadı ınızda otomatik olarak tarayıp kaldırmaya ayarlayın ya da bilgisayarınızın temiz oldu undan emin olmak için taramayı düzenli aralıklarla çalı acak ekilde ayarlayın.

Tarama zamanlamak için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar** > **Zamanlanan tarama** ö elerini seçin.
3. **Zamanlanan tarama**'yı açın.
4. Taramanın ba lamasını istedi iniz zamanı seçin.

Seçenek	Açıklama
Günlük	Bilgisayarınızı her gün tarayın.
Haftalık	Bilgisayarınızı haftanın seçili günlerinde tarayın. Listeden günleri seçin.

Seçenek	Açıklama
Aylık	Bilgisayarınızı ayın seçili günlerinde tarayın. Günleri seçmek için: 1. Gün seçeneklerinden birini seçin. 2. Seçilen günün yanındaki listeden ayın gününü seçin.

5. Seçili günlerde taramayı ne zaman ba latmak istedi inizi seçin.

Seçenek	Açıklama
Ba langıç saati	Taramayı belirtilen zamanda ba latın.
Bilgisayar u süreyle kullanılmadı ında	Taramayı bilgisayarınızı belirtilen zaman süresinde kullanmadıktan sonra ba latın.

Zamanlanan tarama bilgisayarınızı tararken elle tarama ayarlarını kullanır, ancak ar ivleri her zaman tarar ve zarar dosyaları otomatik olarak temizler.

E-postaları tarama

E-posta taraması, size gönderilen e-postalarla zararlı dosyalar almanıza kar ı sizi korur.

E-postaları virüslere kar ı taramak için virüs ve casus yazılım taraması açık olmalıdır.

E-posta taramayı etkinle tirmek için:

1. Ana sayfada Ayarlar'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. Bilgisayar Güvenli i > Virüs ve casus yazılım taraması ö elerini seçin.
3. Zararlı e-posta eklerini kaldır ö esini seçin.
4. Tamam'ı tıklatın.

E-posta iletileri ve ekler ne zaman taranır

Virüs ve casus yazılım taraması, aldı ınız e-postalardaki zararlı içeri i kaldırabilir.

Virüs ve casus yazılım taraması, Microsoft Outlook ve Outlook Express, Microsoft Mail veya Mozilla Thunderbird gibi e-posta programları tarafından alınan zararlı e-posta iletilerini kaldırır. E-posta programınızın POP3 prokolü kullanan posta sunucusundan her e-posta alı ında, ifrelenmemi e-posta iletilerini ve eklerini tarar.

Virüs ve casus yazılım taraması, Hotmail, Yahoo! mail ya da Gmail gibi web tarayıcınızda çalı an e-posta uygulamaları içeren web postasındaki e-posta iletilerini tarayamaz. Zararlı ekleri kaldırmasanız veya web postası kullansanız bile *virüslere* kar ı korunmaya devam edersiniz. E-posta eklerini açtı ınızda, gerçek zamanlı tarama, zararlı ekleri zarar vermeden önce kaldırır.

Not: Gerçek zamanlı tarama arkada larınızı de il, yalnızca bilgisayarınızı korur. Gerçek zamanlı tarama, eki açmadı ınız sürece ekli dosyaları taramaz. Bu da, web postası kullanıyorsanız ve ekini açmadan önce bir iletiyi iletirseniz, arkada larınıza etkilenen bir e-posta iletebilece iniz anlamına gelir.

Tarama sonuçlarını görüntüleme

Virüs ve casus yazılım geçmi i, ürünün buldu u tüm zararlı dosyaları görüntüler.

Bazen, ürün zararlı bir ö e bulundu unda seçti iniz eylemi gerçekle tiremez. Örne in, dosyaları temizlemeyi seçerseniz ve bir dosya temizlenemezse, ürün bu dosyayı karantinaya ta ır. Bu bilgileri virüs ve casus yazılım geçmi inde görüntüleyebilirsiniz.

Geçmi i görüntülemek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i** > **Virüs ve casus yazılım taraması** ö elerini seçin.
3. **Kaldırma geçmi ini görüntüle**'yi tıklatın.

Virüs ve casus yazılım geçmi i a a ıdaki bilgileri görüntüler:

- zararlı dosyanın bulundu u tarih ve saat,
- kötü amaçlı yazılımın adı ve bilgisayarınızdaki konumu,
- gerçekle tirilen eylem.

Dosyalar nasıl taramanın dı ında bırakılır

Bazen, bazı dosyaları veya uygulamaları taramanın dı ında bırakmak isteyebilirsiniz. Dı arıda bırakılan ö eler, siz onları dı arıda bırakılan ö eler listesinden kaldırana kadar taranmaz.

Not: Dı arıda bırakma listeleri, gerçek zamanlı ve elle tarama için ayrı ayrıdır. Örne in, bir dosyayı gerçek zamanlı taramanın dı ında bırakırsanız, elle taramanın da dı ında bırakmadı ınız sürece elle tarama sırasında bu dosya taranır.

Dosya türlerini dı lama

Dosyaları türlerine göre dı arıda bırakırsanız, belirtilen uzantılara sahip dosyalar zararlı içeri e kar ı taranmaz.

Dı arıda bırakmak istedi iniz dosya türünü eklemek veya çıkarmak için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. Dosya türünü gerçek zamanlı veya elle taramanın dı ında bırakmak isteyip istemedi inizi seçin:
   - Dosya türünü gerçek zamanlı taramanın dı ında bırakmak için **Bilgisayar Güvenli i** > **Virüs ve casus yazılım taraması** ö elerini seçin.
   - Dosya türünü gerçek zamanlı taramanın dı ında bırakmak için **Di er ayarlar** > **Elle tarama** ö elerini seçin.
3. **Dosyaları taramanın dı ında bırak**'ı tıklatın.
4. Bir dosya türünü dı lamak için:
   a) **Dosya Türleri** sekmesini seçin.
   b) **u uzantılara sahip dosyaları dı la**'yı seçin.
   c) **Ekle** dü mesinin yanındaki alana, dı lamak istedi iniz dosyaların türünü belirleyen bir dosya uzantısı yazın.

      Uzantısı olmayan dosyaları belirtmek için '.' yazın. Tek bir karakteri belirtmek için '?' joker karakterini, birden çok karakteri belirtmek için '*' joker karakterini kullanabilirsiniz.

      Örne in, yürütülebilir dosyaları dı lamak için bu alana exe yazın.
   d) **Ekle** ö esini tıklatın.
5. Virüs taramalarının dı ında bırakmak istedi iniz di er uzantılar için de önceki adımı yineleyin.
6. **Tamam**'ı tıklatarak **Tarama Dı ı Bırak** ileti im kutusunu kapatın.
7. Yeni ayarları uygulamak için **Tamam**'ı tıklatın.

Seçili dosya türleri gelecekteki taramaların dı ında bırakılır.

Konuma göre dosyaları dı lama

Dosyaları konuma göre dı arıda bıraktı ınızda, belirtilen sürücülerdeki veya klasörlerdeki dosyalar zararlı içeri e kar ı taranmaz.

Dı arıda bırakmak istedi iniz dosya konumları eklemek veya kaldırmak için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. Konumu gerçek zamanlı veya elle taramanın dı ında bırakmak isteyip istemedi inizi seçin:
   - Konumu gerçek zamanlı taramanın dı ında bırakmak için **Bilgisayar** > **Virüs ve casus yazılım taraması** ö elerini seçin.
   - Konumu elle taramanın dı ında bırakmak için **Bilgisayar** > **Elle tarama** ö elerini seçin.
3. **Dosyaları taramanın dı ında bırak**'ı tıklatın.
4. Bir dosyayı, sürücüyü veya klasörü dı lamak için:
   a) **Nesneler** sekmesini seçin.
   b) **Nesneleri dı la (dosyalar, klasörler, ...)** ö esini seçin.
   c) **Ekle** ö esini tıklatın.
   d) Virüs taramasının dı ında bırakmak istedi iniz dosyayı, sürücüyü veya klasörü seçin.

      Not: Bazı sürücüler CD, DVD veya a sürücüleri gibi ta ınabilir sürücüler olabilir. A sürücüleri ve bo ta ınabilir sürücüler dı arıda bırakılamaz.

   e) **Tamam**'ı tıklatın.
5. Ba ka dosya, sürücü veya klasörleri virüs taramasının dı ında bırakmak için önceki adımı yineleyin.
6. **Tamam**'ı tıklatarak **Tarama Dı ı Bırak** ileti im kutusunu kapatın.
7. Yeni ayarları uygulamak için **Tamam**'ı tıklatın.

Seçili dosyalar, sürücüler veya klasörler gelecekteki taramaların dı ında bırakılır.

Dı lanan uygulamaları görüntüleme

Taramanın dı ında bıraktı ınız uygulamaları görüntüleyebilir, gelecekte taramak isterseniz bu uygulamaları dı arıda bırakılan ö eler listesinden kaldırabilirsiniz.

Gerçek zamanlı veya elle tarama casus yazılım veya riskli yazılım gibi davranan ancak güvenli oldu unu bildi iniz bir uygulama algılarsa, ürünün sizi bu yazılımla ilgili daha fazla uyarmaması için yazılımı tarama dı ında bırakabilirsiniz.

Not: Uygulama virüs ya da di er kötü amaçlı yazılımlar gibi davranırsa, tarama dı ında bırakılamaz.

Uygulamaları do rudan dı arıda bırakamazsınız. Yeni uygulamalar yalnızca tarama sırasında siz bu uygulamaları dı arıda bırakırsanız dı arıda bırakılanlar listesinde görünür.

Tarama dı ında bırakılan uygulamaları görüntülemek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. Gerçek zamanlı veya elle taramanın dı ında bırakılan uygulamaları görüntülemek isteyip istemedi inizi seçin:
   - Gerçek zamanlı taramanın dı ında bırakılan uygulamaları görüntülemek için **Bilgisayar** > **Virüs ve casus yazılım taraması** ö elerini seçin.

- Elle taramanın dı ında bırakılan uygulamaları görüntülemek için **Bilgisayar** > **Elle tarama** ö elerini seçin.

3. **Dosyaları taramanın dı ında bırak**'ı tıklatın.
4. **Uygulamalar** sekmesini seçin.

   Not: Yalnızca casus yazılım ve riskli yazılımlar dı lanabilir, virüsler dı lanamaz.

5. Dı arıda bırakılan uygulamayı yeniden taramak isterseniz:
   a) Taramaya eklemek istedi iniz uygulamayı seçin.
   b) **Kaldır**'ı tıklatın.
6. **Tamam**'ı tıklatarak **Tarama Dı ı Bırak** ileti im kutusunu kapatın.
7. Çıkmak için **Tamam**'ı tıklatın.

Karantina nasıl kullanılır

Karantina, zararlı olabilecek dosyalar için güvenli bir depodur.

Karantinaya alınan dosyalar yayılamaz veya bilgisayarınıza zarar veremez.

Zarar vermemeleri için *kötü amaçlı yazılımlar*, *casus yazılımlar* ve *riskli yazılımlar*'ı karantinaya alabilirsiniz. Daha sonra gerekirse uygulamaları veya dosyaları karantinadan geri yükleyebilirsiniz.

Karantinaya alınan bir ö e gerekli de ilse onu silebilirsiniz. Karantinadaki bir ö eyi silmek onu bilgisayarınızdan kalıcı olarak kaldırır.

- Genel olarak, karantinaya alınan *kötü amaçlı yazılımlar*'ı silebilirsiniz.
- Ço u durumda, karantinaya alınan *casus yazılımlar*'ı silebilirsiniz. Karantinaya alınan *casus yazılımlar* yasal bir yazılım programının parçası olabilir ve kaldırıldıklarında asıl program düzgün çalı mayabilir. Programın bilgisayarınızda kalmasını isterseniz, karantinaya alınan *casus yazılımlar*'ı geri yükleyebilirsiniz.
- Karantinaya alınan *riskli yazılım* me ru bir yazılım programı olabilir. Programı kendiniz yükleyip kurduysanız, karantinadan geri yükleyebilirsiniz. *Riskli yazılım* bilginiz dı ında yüklendiyse, büyük olasılıkla kötü amaçlı olarak yüklenmi tir ve kaldırılması gerekir.

Karantinaya alınan ö eleri görüntüleyin

Karantinaya alınan ö eler hakkında daha fazla bilgi görüntüleyebilirsiniz.

Karantinaya alınan ö eler hakkında daha fazla bilgi görüntülemek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i** > **Virüs ve casus yazılım taraması** ö elerini seçin.
3. **Karantinayı görüntüle**'yi tıklatın.
   Karantina sayfası karantinada depolanan toplam ö e sayısını gösterir.
4. Karantinaya alınan ö eler hakkında daha fazla bilgi görüntülemek için **Ayrıntılar**'ı tıklatın.

   çeri i zararlı yazılım adına veya dosya yoluna göre sıralayabilirsiniz.

   Karantinaya alınmı ö elerin türü, bunların adları ve dosyaların yüklü oldu u yol ile birlikte ilk 100 ö enin listesi görüntülenir.
5. Karantinaya alınmı ö e ile ilgili daha fazla bilgi görüntülemek için, **Durum** sütununda ö enin yanındaki simgesini tıklatın.

Karantinaya alınan ö eleri geri yükleme

Karantinaya alınmı ö elerden gereksinim duyduklarınızı geri yükleyebilirsiniz.

Uygulamaları veya dosyaları gerekirse karantinadan geri yükleyebilirsiniz. Hiçbir tehdit olu turmadıklarından emin olmadıkça ö eleri karantinadan geri yüklemeyin. Geri yüklenen ö eler bilgisayarınızda özgün konumlarına geri ta ınırlar.

Karantinaya alınan ö eleri geri yükleme

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i** > **Virüs ve casus yazılım taraması** ö elerini seçin.
3. **Karantinayı görüntüle**'yi tıklatın.
4. Geri yüklemek istedi iniz karantinaya alınmı ö eleri seçin.
5. **Geri Yükle**'yi tıklatın.

DeepGuard nedir

DeepGuard dosyaların içeriklerini ve uygulamaların davranı larını inceler, güvenilmeyen uygulamaları izler.

DeepGuard, bilgisayarınızda de i iklik yapmaya çalı an yeni ve ke fedilmemi *virüsleri*, *solucanlarıve* di er zararlı uygulamaları engeller, üpheli uygulamaların Internet'e eri melerini önler.

DeepGuard, sistemde olası zararlı de i iklikler yapmaya çalı an yeni bir uygulama algıladı ında, uygulamanın güvenli bölgede çalı masına izin verir. Güvenli bölgede, uygulama bilgisayarınıza zarar veremez. DeepGuard uygulamanın yapmaya çalı tı ı de i iklikleri inceler ve buna ba lı olarak, uygulamaların *kötü amaçlı yazılım* olma olasılıklarına karar verir. Uygulamanın *kötü amaçlı yazılım* olma olasılı ı varsa, DeepGuard bu uygulamayı engeller.

DeepGuard'ın algıladı ı olası zararlı sistem de i iklikleri unlardır:

- sistem ayarı (Windows kayıt defteri) de i iklikleri,
- önemli sistem programlarını (örne in, bu ürün gibi güvenlik programlarını) devre dı ı bırakma denemeleri ve
- önemli sistem dosyalarını düzenleme denemeleri.

DeepGuard'ı açma veya kapatma

üpheli uygulamaların bilgisayarınızda olası zararlı sistem de i iklikleri yapmasını önlemek için DeepGuard'ı açık tutun.

Windows XP'niz varsa, DeepGuard'ı açmadan önce Service Pack 2 uygulamasının yüklü oldu undan emin olun.

DeepGuard'ı açmak veya kapatmak için:

1. Ana sayfada **Durum**'u tıklatın.
2. **Bu sayfadaki ayarları de i tir**'i tıklatın.

   Not: Güvenlik özelliklerini kapatmak için yönetici haklarınızın olması gerekir.

3. **DeepGuard**'ı açın veya kapatın.
4. **Kapat**'ı tıklatın.

DeepGuard'ın engelledi i uygulamalara izin verme

DeepGuard'ın hangi uygulamalara izin verdi ini ve hangilerini engelledi ini denetleyebilirsiniz.

Bazen, bir uygulamayı kullanmak isteseniz ve güvenli oldu unu bilseniz bile, DeepGuard güvenli uygulamanın çalı masını engelleyebilir. Bu durum, uygulama zararlı olabilecek sistem de i iklikleri yapmaya çalı tı ı için olu ur. Ayrıca, DeepGuard açılır penceresi görüntülendi inde uygulamayı yanlı lıkla siz de engellemi olabilirsiniz.

DeepGuard'ın engelledi i uygulamaya izin vermek için:

1. Ana sayfada **Araçlar**'ı tıklatın.
2. **Uygulamalar**'ı tıklatın.
   zlenen uygulamalar listesi görüntülenir.
3. zin vermek istedi iniz uygulamayı bulun.

   Not: Listeyi sıralamak için sütun ba lıklarını tıklatabilirsiniz. Örne in, listeyi izin verilen ve reddedilen programlar olarak gruplar halinde sıralamak için **zinler** sütununu tıklatın.

4. **zinler** sütununda **zin Ver**'i seçin.
5. **Kapat**'ı tıklatın.

DeepGuard uygulamanın sistem de i iklikleri yapmasına yeniden izin verir.

DeepGuard'ı uyumluluk modunda kullanma

Maksimum koruma için, DeepGuard çalı an programları geçici olarak de i tirir. Bazı programlar, bozulup bozulmadıkları veya de i tirilip de i tirilmediklerini ve bu özellikle uyumlu olup olmadıklarını denetler. Örne in, hile önleme araçları bulunan çevrimiçi oyunlar, çalı ırken herhangi bir ekilde de i tirilip de i tirilmediklerini denetler. Bu gibi durumlarda, uyumluluk modunu açabilirsiniz.

Uyumluluk modunu açmak için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

   Not: Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i** > **DeepGuard** ö elerini seçin.
3. **Uyumluluk modunu kullan** ö esini seçin.
4. **Tamam**'ı tıklatın.

üpheli davranı uyarılarıyla ne yapmak gerekir

DeepGuard güvenilmeyen uygulamaları izler. zlenen bir uygulama Internet' eri meyi denerse, sisteminizde de i iklik yapmaya çalı ırsa ya da üpheli davranırsa, DeepGuard bu uygulamayı engeller.

DeepGuard ayarlarında **üpheli davranı hakkında beni uyar** seçene i belirledi inizde, DeepGuard, olası zararlı bir uygulama algıladı ında veya tanınmayan bir uygulamayı ba lattı ınızda sizi uyarır.

DeepGuard'ın engelledi i bir uygulamayla ne yapmak istedi inizde karar vermek için:

1. Programla ilgili daha fazla bilgi görüntülemek için **Ayrıntılar**'ı tıklatın.
   Ayrıntılar bölümünde unları görürsünüz:
   - uygulamanın konumu,
   - Gerçek Zamanlı Koruma A ı'nda uygulamanın tanınırlı ı,
   - uygulamanın ne kadar yaygın oldu u.
2. DeepGuard'ın engelledi i uygulamaya güvenip güvenmedi inize karar verin:

- Uygulamayı engellemek istemiyorsanız **Uygulamaya güveniyorum. Devam etmesine izin ver.** seçene ini belirleyin.

  u durumlarda uygulamanın güvenli olması olasıdır:

  - DeepGuard, sizin yaptı ınız bir eylem sonucu uygulamayı engelledi,
  - uygulamayı biliyorsunuz ya da
  - uygulamayı güvenilir bir kaynaktan edindiniz.

- Uygulamanın engellenmesini istiyorsanız **Uygulamaya güvenmiyorum. Engelli kalmasını sa la.** seçene ini belirleyin.

  Uygulama u durumlardaysa güvenli olmayabilir:

  - Uygulama yaygın de il,
  - uygulama tanınmıyor ya da
  - uygulamayı bilmiyorsunuz.

3. üpheli bir uygulamayı analize göndermek istiyorsanız:

a) **Uygulamayı F-Secure'a bildir**'i tıklatın.
Ürün, gönderme ko ullarını görüntüler.

b) Ko ulları kabul ediyorsanız ve örne in göndermek istiyorsanız **Kabul Et**'i tıklatın.

u durumlarda bir örnek göndermenizi öneririz:

- DeepGuard güvenli oldu unu bildi iniz bir uygulamayı engelledi ya da
- uygulamanın *kötü amaçlı yazılım* olabilece inden üphelendiniz.